

551,844

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2004 年 10 月 28 日 (28.10.2004)

PCT

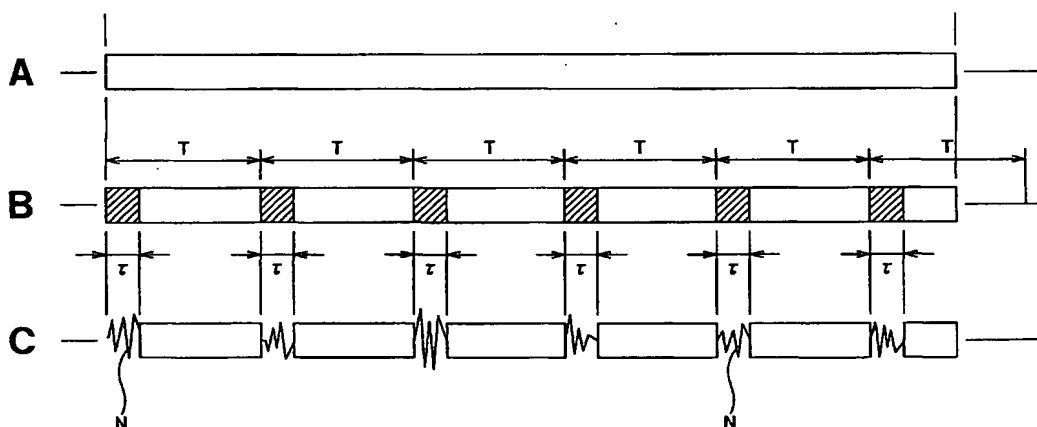
(10) 国際公開番号  
WO 2004/093073 A1

- (51) 国際特許分類: G11B 20/10, 20/12, G09C 1/00
- (21) 国際出願番号: PCT/JP2004/004288
- (22) 国際出願日: 2004 年 3 月 26 日 (26.03.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願2003-107278 2003 年 4 月 11 日 (11.04.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 小池 隆 (KOIKE, Takashi) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 岩津 健 (IWATSU, Takeshi) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP). 木村 学 (KIMURA, Manabu) [JP/JP]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo (JP).
- (74) 代理人: 小池 晃, 外 (KOIKE, Akira et al.); 〒1000011 東京都千代田区幸町一丁目 1 番 7 号 大和生命ビル 11 階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- 添付公開書類:  
— 国際調査報告書

[続葉有]

(54) Title: DIGITAL DATA STORAGE/REPRODUCTION METHOD AND DEVICE

(54) 発明の名称: デジタルデータの保存・再生方法及び装置



(57) Abstract: There is provided a digital data storage method. For digital data whose content is changed with time lapse, a predetermined span  $\tau$  is partially encrypted for each predetermined time  $T$ . Here, the encryption is performed so that the ratio of the span  $\tau$  of the encryption part with respect to the time  $T$  and the span  $\tau$  occupied by the encryption part are sufficiently small. The digital data encrypted is stored.

(57) 要約: 本発明は、デジタルデータの保存方法であり、内容が時間とともに変化するデジタルデータに対して、所定の時間  $T$  毎に所定の期間  $\tau$  ずつ部分的に暗号化を行う。このとき、暗号化部分の期間  $\tau$  の所定の時間  $T$  に対する割り合い、及び暗号化部分の占める期間  $\tau$  が、十分に小さくなるように暗号化を行う。この暗号化のされたデジタルデータを保存する。

WO 2004/093073 A1



2文字コード及び他の略語については、定期発行される  
各PCTガゼットの巻頭に掲載されている「コードと略語  
のガイダンスノート」を参照。

## 明細書

## デジタルデータの保存・再生方法及び装置

## 技術分野

本発明は、オーディオ信号などのデジタルデータを保存するための保存方法及び保存装置、さらにデータ再生方法及び再生装置に関する。

本出願は、日本国において２００３年４月１１日に出願された日本特許出願番号２００３－１０７２７８を基礎として優先権を主張するものであり、この出願は参照することにより、本出願に援用される。

## 背景技術

デジタル処理やネットワーク技術の進展にともない、デジタルオーディオデータを放送やネットワークなどを通じてユーザに配信する技術が提供されている。この種の技術に用いられるオーディオ機器として、特開２００３－３００１８公報に記載されるようなオーディオサーバ提案されている。この公報に記載されるオーディオサーバは、配信されたデジタルオーディオデータを内蔵のハードディスク装置（ＨＤＤ：Hard Disk Drive）に一旦保存し、これを好きなときに取り出せるようにしたものである。また、オーディオサーバとして、特開２００１－２４３７０５公報に記載されるようなものが提案されている。この公報に記載される装置は、デジタルオーディオデータを暗号化して保存し、認証を受けたときのみ、その暗号化されたデジタルオーディオデータを復号化して出力するようにしたものである。

ところで、オーディオサーバにおいては、そのサーバに組み込まれているソフトウェアにしたがった処理しか実行できないので、内蔵のＨＤＤに保存されたデジタルオーディオデータをＣＤ－Ｒ（CD Recordable）などにコピーすることはできない。しかし、オーディオサーバから内蔵のＨＤＤを物理的に取り出してパー

ソナルコンピュータに接続すれば、そのHDDに保存されているデジタルオーディオデータを、他のHDDやCD-Rなどにコピーすることができ、著作権者の権利を守れなくなってしまう。

そこで、オーディオサーバにおいて、配信されたデジタルオーディオデータを暗号化してから内蔵のHDDに取り込むことが考えられている。つまり、そのようにすれば、認証を受けたオーディオサーバにおいては、その暗号化されたデジタルオーディオデータを復号化することにより音楽などを正常に聴くことができる。

しかし、その内蔵のHDDを取り出してパーソナルコンピュータに接続しても、暗号化されたデジタルオーディオデータを復号化することはできないので、結果として、著作権を保護することができる。

ところが、家庭用のオーディオサーバは、概して使用しているCPU（Central Processing Unit）の処理能力が低いので、再生時、CPUによりデジタルオーディオデータを連続して復号化することができない。もちろん、CPUとして処理能力の高いものを使用すれば、あるいは復号化専用のIC（Integrated Circuit）を設ければ、再生時、暗号化されたデジタルオーディオデータを連続して復号化することができるが、その場合には、サーバのコストが上昇してしまう

## 発明の開示

本発明の目的は、従来の技術が有する問題点を解消することができる新規なデジタルデータの保存方法及び保存装置並びにデータ再生方法及び再生装置、さらにはデジタルデータを記録するための記録媒体を提供することにある。

本発明は、デジタルデータの保存方法であり、デジタルデータのうち一部のデジタルデータに対して暗号化を施し、この暗号化を施したデジタルデータと、暗号化を施さない非暗号化デジタルデータとを保存する。

本発明に係るデジタルデータの保存方法は、さらに、デジタルデータを所定のデータサイズに分割し、分割されたデジタルデータ毎に、その一部のデジタルデータに対して暗号化を施して暗号デジタルデータを得る。

また、本発明は、データ保存装置であり、デジタルデータのうち一部のデジタルデータに対して暗号化を施す暗号化手段と、この暗号化手段により暗号化を施した暗号デジタルデータと、暗号化を施さない非暗号デジタルデータとを保存する保存手段とを備える。

本発明に係るデータ保存装置は、さらに、デジタルデータを所定のデータサイズに分割する分割手段を備え、暗号化手段は、分割手段により分割されたデジタルデータ毎に、その一部のデジタルデータに対して暗号化を施して暗号化デジタルデータを得る。

さらに、本発明は、デジタルデータの記録媒体であり、デジタルデータのうちの一部のデジタルデータに対して暗号化を施して得られた暗号デジタルデータと、暗号化を施さない非暗号デジタルデータとが記録されている。

ここで、デジタルデータは所定のデータサイズに分割され、分割されたデジタルデータ毎に、その一部のデジタルデータに対して暗号化を施したデジタルデータが記録されている。

さらにまた、本発明は、データ再生方法であり、暗号化を施された暗号デジタルデータと、暗号化を施されていない非暗号デジタルデータとからなるデジタルデータを取り込み、このデジタルデータから上記暗号デジタルデータを取り出して、この暗号デジタルデータを復号し、復号化された復号デジタルデータと、デジタルデータから取り出される非暗号デジタルデータとを再生データとして出力する。

さらにまた、本発明は、データ再生装置であり、暗号化を施された暗号デジタルデータと、暗号化を施されていない非暗号化デジタルデータとからなるデジタルデータを入力する入力手段と、この入力手段で入力されるデジタルデータから暗号デジタルデータを取り出して、この暗号デジタルデータを復号化する復号手段と、復号手段で復号された復号デジタルデータと、デジタルデータから取り出される非暗号デジタルデータとを再生データとして出力する再生手段とを備える。

ここで、デジタルデータは、所定のデータサイズ毎に暗号デジタルデータと非暗号デジタルデータとからなり、復号手段は、所定のデータサイズ毎に暗号デジタルデータを取り出して、この暗号デジタルデータを復号化する。

また、入力手段は、デジタルデータとともに、暗号デジタルデータの位置を示す情報を取り込み、復号手段は、取り込まれた位置情報に基づいて暗号デジタルデータを取り出して復号化する。

本発明に係るデータ再生装置は、さらに、暗号デジタルデータの位置を示す情報を暗号化した暗号位置情報を復号化する第2の復号手段を備え、入力手段は、デジタルデータとともに、暗号位置情報を取り込み、復号手段は、第2の復号手段で復号化された暗号デジタルデータの位置を示す情報に基づいて暗号デジタルデータを取り出して復号化する。

本発明の更に他の目的、本発明によって得られる具体的な利点は、以下において図面を参照して説明される実施の形態の説明から一層明らかにされるであろう

#### 図面の簡単な説明

図1は、本発明を適用したオーディオサーバを示すブロック図である。

図2Aは暗号化されるデジタルオーディオデータを模式的に示す図であり、図2Bは暗号化回路から出力されるデジタルオーディオデータを模式的に示す図であり、図2Cは暗号化部分がノイズ音となったディスクオーディオデータを模式的に示す図である

図3は、本発明が適用されたCDプレーヤを示すブロック図である。

図4は、任意の期間 $T_i$  ( $i=1\sim n$ ) 毎に、任意の期間 $\tau_i$ ずつ暗号化したデジタルオーディオデータを模式的に示す図である。

図5は、デジタルオーディオデータを任意の期間 $T_i$  ( $i=1\sim n$ ) 毎に、任意の期間 $\tau_i$ ずつ暗号化するとき用いる任意の期間 $T_i$  ( $i=1\sim n$ ) と任意の期間 $\tau_i$  のテーブルを示す。

#### 発明を実施するための最良の形態

以下、本発明を適用した実施の形態について、図面を参照しながら詳細に説明する。

まず、本発明をオーディオサーバに適用した例を挙げて説明する。このオーディオサーバ 30 には、図 1 に示すように、各種のオーディオ信号のソース 10 とオーディオ出力装置 20 が接続されている。

本発明に係るオーディオサーバ 30 に用いられるソース 10 は、ネットワーク、CD プレーヤ、デジタル放送のチューナなどの信号源であり、オーディオ信号をデジタルデータ、すなわち、デジタルオーディオデータの状態で提供するものである。出力装置 20 は、図示はしないが、D/A (Digital to Analog) コンバータ回路やスピーカなどを有し、ソース 10 あるいはオーディオサーバ 30 からデジタルオーディオデータが供給されると、そのデジタルオーディオデータを音響として出力するものである。

さらに、オーディオサーバ 30 は、ユーザの指示にしたがって、ソース 10 から出力されるデジタルオーディオデータを保存し、あるいはその保存したデジタルオーディオデータを再生して出力装置 20 に出力する。このため、オーディオサーバ 30 はマイクロコンピュータにより構成されている。

すなわち、オーディオサーバ 30 は、各種のプログラムを実行する CPU (Central Processing Unit) 31 と、ROM (Read Only Memory) 32 と、ワークエリア用の RAM (Random Access Memory) 33 と、ユーザインタフェース 34 とを有し、これらがシステムバス 39 を通じて互いに接続されている。この場合、ROM 32 は、CPU 31 が実行する各種のプログラムが書き込まれている。また、ユーザインタフェース 34 は、ユーザにより操作される各種の操作キー（操作スイッチ）、及びこのオーディオサーバ 30 の状態などを表示するディスプレイを含む。

さらに、ソース 10 が入力インタフェース 35 を通じてシステムバス 39 に接続され、システムバス 39 が出力インタフェース 36 を通じて出力装置 20 に接続される。また、大容量の保存手段として、例えばハードディスク装置 (HDD : Hard Disk Drive) 38 が設けられ、この HDD 38 が HDC (Hard Disk Controller) 37 を通じてシステムバス 39 に接続されている。なお、HDD 38 は、一般のパーソナルコンピュータなどにおいて使用されている HDD とすることができる。

また、システムバス 39 には、暗号化回路 41、復号化回路 42 及び認証回路 43 が接続される。ただし、この場合、暗号化回路 41、復号化回路 42 及び認証回路 43 は、ソフトウェアにより構成されるものであり、すなわち、CPU 31 が ROM 32 のプログラムを実行することにより実現されるものである。したがって、データ保存時の暗号化回路 41 の暗号化処理及びデータ取出時の復号化回路 42 の復号化処理は、そのデータの保存処理及びデータの取出処理と並行して実行されることになるので、CPU 31 にとって負荷となる。なお、暗号化回路 41 の暗号方式は、もとのデジタルデータとの相関がほとんどなくランダムノイズに近い暗号文データが作製される方式、例えば DES (Data Encryption Standard) 暗号化方式とされる。

さらに、認証回路 43 は、例えば、出力装置 20 をチェックし、これが予め設定されている正当な出力装置であるときのみ、出力装置 20 へのデジタルオーディオデータの出力を許可するためのものである。

このような構成において、オーディオサーバ 30 がソース 10 から出力されるデジタルオーディオデータを保存する場合には、そのデジタルオーディオデータは、入カインタフェース回路 35 を通じて暗号化回路 41 に供給され、図 2A～図 2C に示すように暗号化される。

ここで、図 2A は、暗号化回路 41 に入力されるデジタルオーディオデータを示し、図 2B は、暗号化回路 41 から出力されるデジタルオーディオデータを示す。そして、暗号化回路 41 の出力デジタルオーディオデータにおいては、斜線を付けた部分だけが暗号化されている。すなわち、暗号化回路 41 においては、もとのデジタルオーディオデータのうち、所定の周期  $T$  毎に、所定の期間  $\tau$  の部分（斜線部分）だけが暗号化される。この場合、値  $T$ 、 $\tau$  は、暗号化回路 41 の一部として、ROM 32 のプログラムに用意される。また、一例として、 $T = 23$  m秒、 $\tau = 1$  m秒とされる。

そして、この部分的に暗号化されたデジタルオーディオデータが HDC 37 を通じて HDD 38 に書き込まれる。

一方、オーディオサーバ 30 に保存されているデジタルオーディオデータを使用する場合には、まず、認証回路 43 により出力装置 20 に対する認証処理が行



われる。そして、その認証処理の結果、出力装置 20 が正当な出力装置のときには、HDC 37 を通じて HDD 38 から目的とするデジタルオーディオデータが読み出され、この読み出されたデジタルオーディオデータが復号化回路 42 に供給され、周期  $T$  毎の期間  $\tau$  の暗号化部分が復号化されてもとのデジタルオーディオデータが取り出され、このデジタルオーディオデータが出力インタフェース回路 36 を通じて出力装置 20 に供給され、音響として再生される。

なお、出力装置 20 に対する認証処理の結果、出力装置 20 が正当な出力装置ではないときには、HDD 38 からのデジタルオーディオデータの読み出しは行われず、したがって、出力装置 20 へのデジタルオーディオデータの出力は許可されない。

こうして、上述のオーディオサーバ 30 によれば、デジタルオーディオデータを保存し、これを必要なときに取り出すことができる。そして、その場合、オーディオサーバ 30 から HDD 38 を物理的に取り出してパーソナルコンピュータに接続することにより、HDD 38 に保存されているデジタルオーディオデータを他の HDD や CD-R などにコピーして再生することができる。

しかし、他の HDD や CD-R (CD Recordable) にコピーしたデジタルオーディオデータは、図 2B に示すように、周期  $T$  毎に期間  $\tau$  の暗号化部分を有するとともに、この暗号化部分のデジタルオーディオデータは、パーソナルコンピュータにおいては復号化されることなく音響として再生されるので、図 2C に示すように、その暗号化部分はノイズ音  $N$  として出力される。

すなわち、HDD 38 のデジタルオーディオデータを他の HDD や CD-R などにコピーしても、その再生音には周期的にノイズ音が含まれるので、音楽などの再生に支障を来し、実用にならない。したがって、著作権者の権利を守ることができる。

しかも、CPU 31 が、暗号化回路 41 の暗号化処理及び復号化回路 42 の復号化処理を実行するのは、周期  $T$  毎に期間  $\tau$  であり、つまり、全体の  $\tau/T$  の期間であるから、この割り合い  $\tau/T$  及び値  $\tau$  を予め小さくしておくことにより、暗号化処理及び復号化処理に対する CPU 31 の負担を軽減することができ、したがって、CPU 31 として処理能力の高いものを必要としない。あるいは、C

P U 3 1 の処理能力が低くても、その暗号化処理及び復号化処理を実行することができる。また、これにより、暗号化や復号化のために専用の I C (Integrated Circuit) を設ける必要もない。したがって、オーディオサーバ 3 0 のコストを低減することができる。

図 3 は、この発明を C D (Compact Disc) 及び C D プレーヤに適用した場合の一例を示す。まず、C D の作製時 (記録時)、アナログオーディオ信号 L、R が A/D (Analog to Digital) コンバータ回路 5 1 に供給されてデジタルオーディオデータに A/D 変換され、このデジタルオーディオデータが暗号化回路 5 2 に供給される。また、信号形成回路 5 4 から周期 T 毎に期間  $\tau$  を示す信号が暗号化回路 5 2 に供給される。こうして、暗号化回路 5 2 において、これに供給されたデジタルオーディオデータは、図 2 B に斜線で示すように、周期 T 毎に期間  $\tau$  ずつ暗号化される。

そして、この部分的に暗号化されたデジタルオーディオデータが、記録回路 5 3 に供給されてエラー訂正のエンコード及び E F M 変調などの処理が行われ、この E F M 信号が C D の原盤に記録される。なお、このとき、信号形成回路 5 4 から値 T、 $\tau$  を示すデータが取り出され、このデータが暗号化回路 5 2 により暗号文データに暗号化されてから記録回路 5 3 に供給され、値 T、 $\tau$  の暗号文データが C D の原盤にサブコードとして記録される。こうして、図 2 B に示すように部分的に暗号化されたデジタルオーディオデータを有する C D 6 0 がその原盤から作製される。

C D 6 0 の再生は、C D プレーヤ 7 0 により行われる。すなわち、光学ピックアップ 7 1 により C D 6 0 から E F M (Eight to Fourteen Modulation) 信号が再生され、この再生された E F M 信号が D S P (Digital Signal Processor) 7 2 の再生回路 7 2 1 に供給される。この再生回路 7 2 1 及び次段の復号化回路 7 2 2 は、D S P 7 2 が実行するプログラムにより実現される。また、この D S P 7 2 には、この C D プレーヤ 7 0 の全体の動作などを制御するマイクロコンピュータ 8 0 が接続される。

そして、再生回路 7 2 1 において、記録回路 5 3 とは相補の処理が行われ、すなわち、E F M 信号の復調及びエラー訂正などが行われ、部分的に暗号化された

デジタルオーディオデータと、暗号化されたサブコードとが取り出され、そのデジタルオーディオデータが復号化回路 722 に供給される。また、再生回路 721 により取り出されたサブコードがマイクロコンピュータ 80 に供給され、CD 60 に対して、予め認証を受けているときには、もとの値  $T$ 、 $\tau$  のデータが復号化されて取り出され、この値  $T$ 、 $\tau$  のデータが復号化回路 722 に供給される。

そして、復号化回路 722 において、値  $T$ 、 $\tau$  を使用してデジタルオーディオデータの暗号化部分が復号化されてもとのデジタルオーディオデータとされる。そして、このデジタルオーディオデータが D/A (Digital to Analog) コンバータ回路 73 に供給されてもとのアナログオーディオ信号  $L$ 、 $R$  に D/A 変換されて取り出される。

こうして、上述の CD 60 は、認証を受けた CD プレーヤ 70 で再生した場合には、正常に再生をすることができる。しかし、認証を受けていない CD プレーヤで再生した場合には、CD 60 から再生されたデジタルオーディオデータの暗号化部分が復号化されることなく音響として再生されるので、その暗号化部分はノイズ音として出力される。したがって、CD 60 を認証を受けていない CD プレーヤで再生した場合には、その再生に支障を来し、実用にならないので、著作権者の権利を守ることができる。

しかも、DSP 72 が復号化回路 722 の復号化処理を実行するのは、全体の  $\tau/T$  の期間であるから、この割り合い  $\tau/T$  及び値  $\tau$  を予め小さくしておくことにより、復号化処理に対する DSP 72 の負担を軽減することができ、DSP 72 として処理能力の高いものを必要としない。あるいは DSP 72 の処理能力が低くても、復号化処理を実行することができる。また、これにより、復号化のために専用の IC を設ける必要もない。したがって、CD プレーヤ 70 のコストを抑えることができる。

さらに、CD 60 の正規のユーザであれば、CD 60 を CD-R などにコピーしても再生をすることができるので、CD 60 のバックアップを取ることができる。

なお、上述において、オーディオサーバ 30 あるいは CD プレーヤ 70 が認証を受ける方法、あるいは暗号化部分を復号化するときに許可を受ける方法は、任

意である。また、上述においては、デジタルオーディオデータが周期 $T$ 毎に期間 $\tau$ ずつ暗号化部分を有する場合であるが、図4に示すように、デジタルオーディオデータに対して、任意の期間 $T_i$  ( $i=1\sim n$ ) 毎に、任意の期間 $\tau_i$ ずつ暗号化部分（斜線図示）とすることもできる。特に、デジタルオーディオデータの内容が音楽の場合、期間 $T_i$ を数十小節のフレーズにしたり、期間 $\tau_i$ をサビの部分や音量の小さくなる部分に割り当てると効果的である。

そして、その場合には、図1に示すオーディオサーバ30であれば、値 $T_i$ 、 $\tau_i$ を、例えば図5に示すようなテーブル（テーブルに相当するものを含む）の形式でROM32に用意し、あるいは図3に示すCDプレーヤ70であれば、そのテーブルをサブトラックに用意することができる。

また、図1に示すオーディオサーバ30においては、値 $T$ 、 $\tau$ （あるいは $T_i$ 、 $\tau_i$ ）をROM32に設けるとしたが、図3に示すCD60と同様、ソース10から得るようにすることもでき、その場合には、値 $T$ 、 $\tau$ を暗号化しておき、認証を受けたとき、その暗号化された値 $T$ 、 $\tau$ を復号化してデジタルオーディオデータの暗号化部分の復号化に使用することもできる。

さらに、上述においては、対象となるデジタルデータがデジタルオーディオデータの場合であるが、時間とともに連続的に変化する内容のデジタルデータであれば、ビデオ信号や動画などのデジタルデータであってもよい。また、HDD38の代わりに不揮発性メモリとすることもできる。

なお、本発明は、図面を参照して説明した上述の実施例に限定されるものではなく、添付の請求の範囲及びその主旨を逸脱することなく、様々な変更、置換又はその同等のものを行うことができることは当業者にとって明らかである。

#### 産業上の利用可能性

上述したように、本発明によれば、デジタルデータを保存したHDDを他のパーソナルコンピュータなどにより使用しても、デジタルデータは部分的に暗号化してあり、その暗号化部分はノイズとして再生されるので、実用的な再生とすることができず、著作権者の権利を守ることができる。

しかも、その暗号化部分を予め小さくしておくことにより、再生に使用するCPUとして処理能力の高いものを必要としない、復号化のために専用のICを設ける必要もないので、装置のコストを低減することができる

## 請求の範囲

1. デジタルデータのうち一部のデジタルデータに対して暗号化を施し、  
上記暗号化を施したデジタルデータと、暗号化を施さない非暗号化デジタルデータとを保存する  
ことを特徴とするデジタルデータの保存方法。
2. 上記暗号化を施す部分のデータサイズは、デジタルデータのデータサイズよりも十分に小さいことを特徴とする請求の範囲第1項記載のデジタルデータの保存方法。
3. デジタルデータを所定のデータサイズに分割し、分割されたデジタルデータ毎に、その一部のデジタルデータに対して暗号化を施して暗号デジタルデータを得ることを特徴とする請求の範囲第1項記載のデジタルデータの保存方法。
4. 上記暗号デジタルデータの位置を示す情報を、上記暗号デジタルデータ及び非暗号デジタルデータとともに保存することを特徴とする請求の範囲第1項記載のデジタルデータの保存方法。
5. 上記デジタルデータの位置を示す情報を暗号化し、この暗号化された位置情報を、上記暗号デジタルデータ及び非暗号化デジタルデータとともに保存するようにしたことを特徴とする請求の範囲第4項記載のデジタルデータの保存方法。
6. デジタルデータのうち一部のデジタルデータに対して暗号化を施す暗号化手段と、  
上記暗号化手段により暗号化を施した暗号デジタルデータと、暗号化を施さない非暗号デジタルデータとを保存する保存手段と  
を備えることを特徴とするデータ保存装置。
7. 上記暗号化手段が暗号化を施す部分のデータサイズは、デジタルデータのデータサイズよりも十分に小さいことを特徴とする請求の範囲第6項記載のデータ保存装置。
8. デジタルデータを所定のデータサイズに分割する分割手段を備え、上記暗号化手段は、上記分割手段により分割されたデジタルデータ毎に、その一部のデジタルデータに対して暗号化を施して暗号化デジタルデータを得ることを特徴とする

る請求の範囲第 6 項記載のデータ保存装置。

9. 上記保存手段は、上記暗号化デジタルデータの位置を示す情報を、上記暗号デジタルデータ及び非暗号デジタルデータとともに保存することを特徴とする請求の範囲第 6 項記載のデータ保存装置。

10. 上記暗号デジタルデータの位置を示す情報を暗号化して暗号位置情報を得る第 2 の暗号化手段を備え、上記第 2 の暗号化手段により得られた上記暗号位置情報を、上記暗号デジタルデータ及び非暗号デジタルデータとともに保存することを特徴とする請求の範囲第 9 項記載のデータ保存装置。

11. デジタルデータのうちの一部のデジタルデータに対して暗号化を施して得られた暗号デジタルデータと、暗号化を施さない非暗号デジタルデータとが記録されていることを特徴とする記録媒体。

12. 上記暗号化を施した部分のデータサイズは、デジタルデータのデータサイズよりも十分に小さいことを特徴とする請求の範囲第 11 項記載の記録媒体。

13. デジタルデータは所定のデータサイズに分割され、分割されたデジタルデータ毎に、その一部のデジタルデータに対して暗号化を施したデジタルデータが記録されていることを特徴とする請求の範囲第 11 項記載の記録媒体。

14. 上記暗号デジタルデータの位置を示す情報が、上記暗号デジタルデータ及び非暗号デジタルデータとともに記録されていることを特徴とする請求の範囲第 11 項記載の記録媒体。

15. 上記暗号デジタルデータの位置を示す情報を暗号化し、この暗号化された位置情報が、上記暗号デジタルデータ及び非暗号デジタルデータとともに記録されていることを特徴とする請求の範囲第 14 項記載の記録媒体。

16. 暗号化を施された暗号デジタルデータと、暗号化を施されていない非暗号デジタルデータとからなるデジタルデータを取り込み、

このデジタルデータから上記暗号デジタルデータを取り出して、この暗号デジタルデータを復号し、

復号化された復号デジタルデータと、上記デジタルデータから取り出される上記非暗号デジタルデータとを再生データとして出力する

ことを特徴とするデータ再生方法。

17. 上記デジタルデータは、所定のデータサイズ毎に上記暗号デジタルデータと上記非暗号デジタルデータとからなり、上記所定のデータサイズ毎に上記暗号デジタルデータを取り出して、この暗号デジタルデータを復号化することを特徴とする請求の範囲第16項記載のデータ再生方法。

18. 上記デジタルデータとともに、上記暗号デジタルデータの位置を示す情報を取り込み、上記取り込まれた位置情報に基づいて上記暗号デジタルデータを取り出して復号化することを特徴とする請求の範囲第16項記載のデータ再生方法。

19. 上記デジタルデータとともに、上記暗号デジタルデータの位置を示す情報を暗号化した暗号位置情報を取り込み、上記暗号位置情報を復号化し、この復号化された上記暗号デジタルデータの位置を示す情報に基づいて上記暗号デジタルデータを取り出して復号化することを特徴とする請求の範囲第18項記載のデータ再生方法。

20. 暗号化を施された暗号デジタルデータと、暗号化を施されていない非暗号化デジタルデータとからなるデジタルデータを入力する入力手段と、

上記入力手段で入力されるデジタルデータから上記暗号デジタルデータを取り出して、この暗号デジタルデータを復号化する復号手段と、

上記復号手段で復号された復号デジタルデータと、上記デジタルデータから取り出される上記非暗号デジタルデータとを再生データとして出力する再生手段と、  
を備えることを特徴とするデータ再生装置。

21. 上記デジタルデータは、所定のデータサイズ毎に上記暗号デジタルデータと上記非暗号デジタルデータとからなり、上記復号手段は、上記所定のデータサイズ毎に上記暗号デジタルデータを取り出して、この暗号デジタルデータを復号化することを特徴とする請求の範囲第20項記載のデータ再生装置。

22. 上記入力手段は、上記デジタルデータとともに、上記暗号デジタルデータの位置を示す情報を取り込み、上記復号手段は、上記取り込まれた位置情報に基づいて上記暗号デジタルデータを取り出して復号化することを特徴とする請求の範囲第20項記載のデータ再生装置。

23. 上記暗号デジタルデータの位置を示す情報を暗号化した暗号位置情報を復号化する第2の復号手段をさらに備え、上記入力手段は、上記デジタルデータと



ともに、上記暗号位置情報を取り込み、上記復号手段は、上記第2の復号手段で復号化された上記暗号デジタルデータの位置を示す情報に基づいて上記暗号デジタルデータを取り出して復号化することを特徴とする請求の範囲第22項データ再生装置。

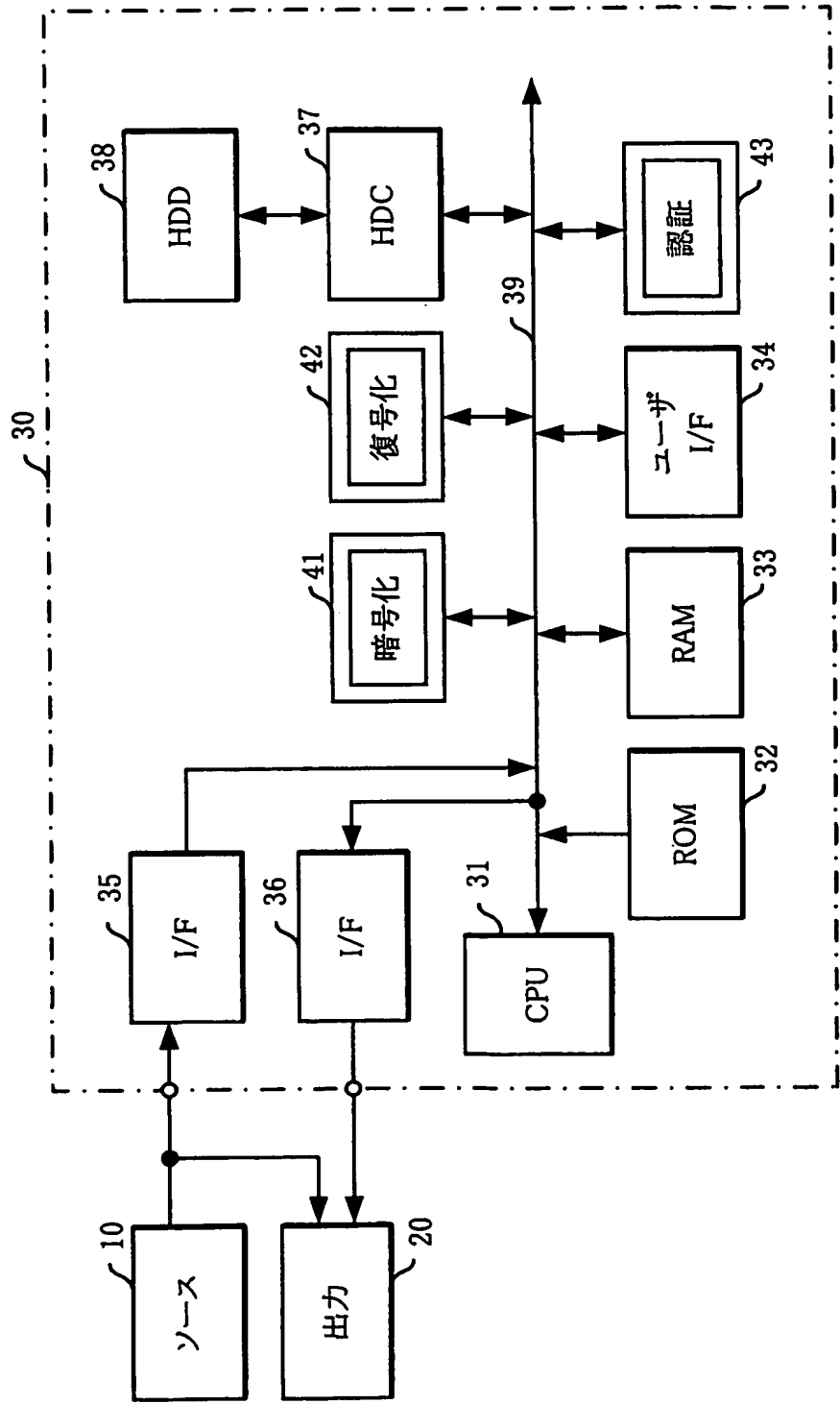
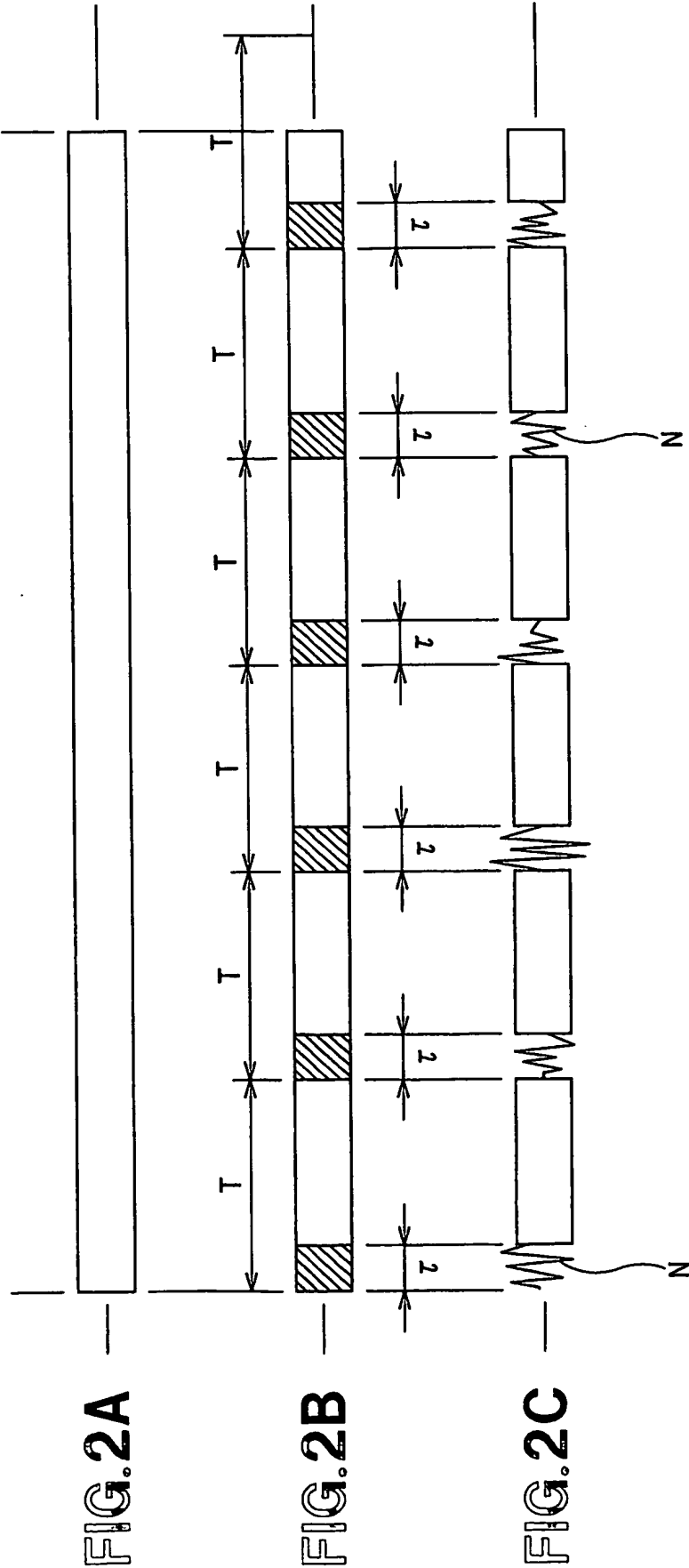


FIG.1



3/5

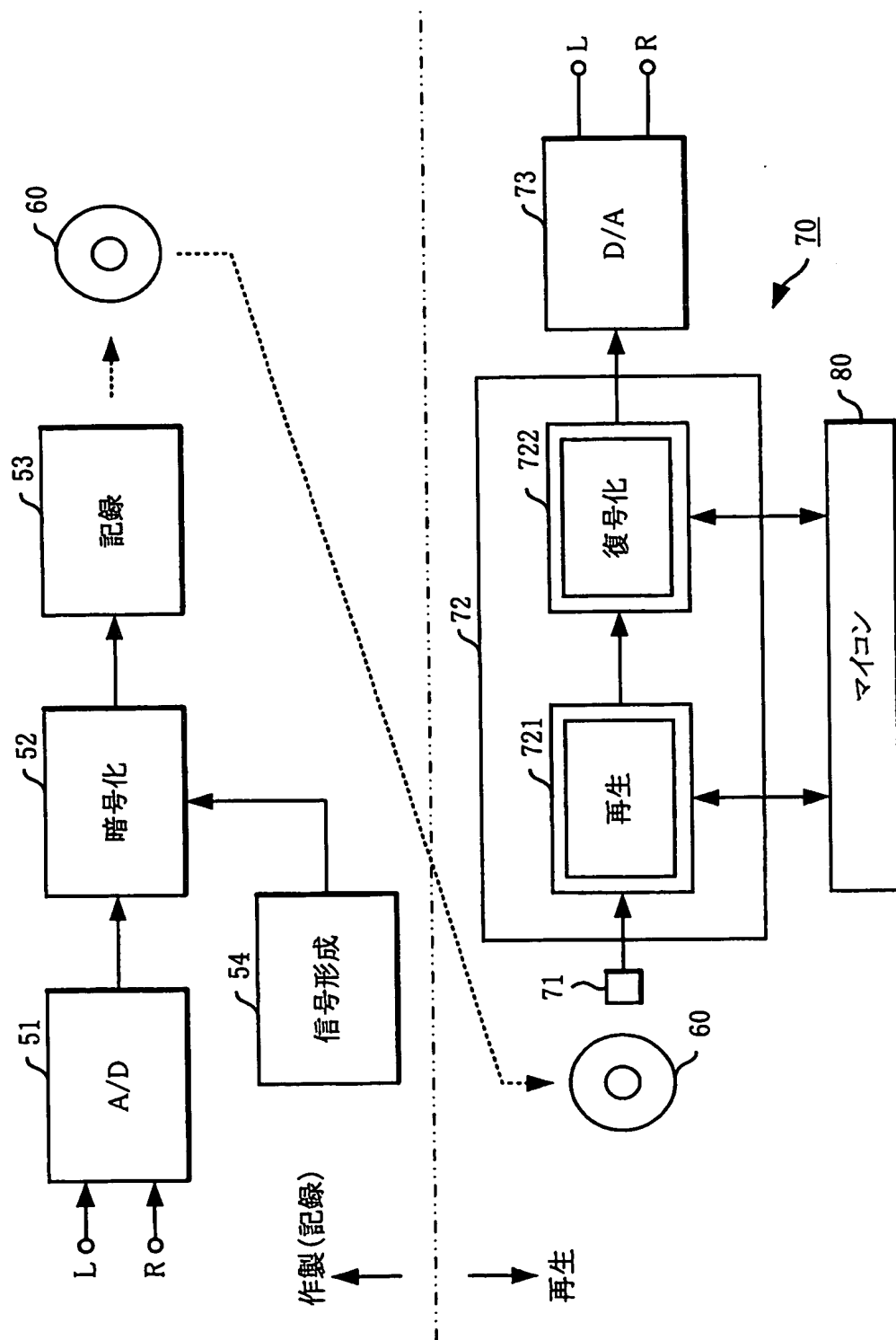


FIG.3

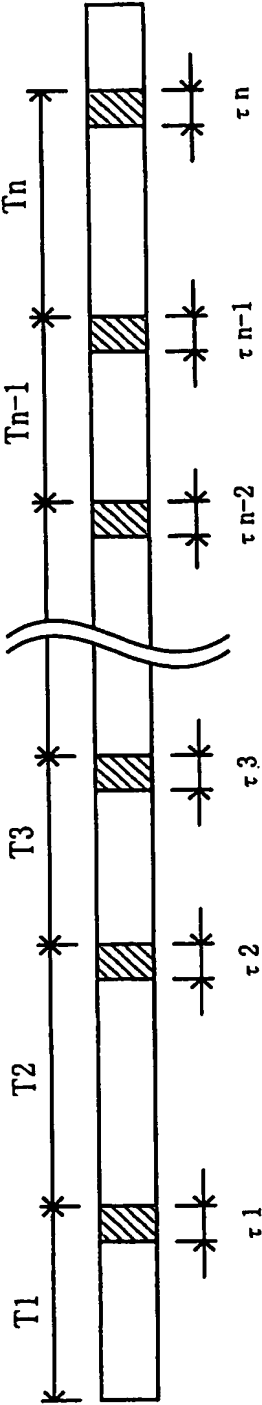


FIG.4

	期間(位置)	期間
暗号化部分1	T1	$\tau_1$
暗号化部分2	T2	$\tau_2$
暗号化部分3	T3	$\tau_3$
$\vdots$	$\vdots$	$\vdots$
暗号化部分n	Tn	$\tau_n$

FIG.5

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/004288

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G11B20/10, G11B20/12, G09C1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G11B20/10, G11B20/12, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-158654 A (Hitachi, Ltd.), 31 May, 2002 (31.05.02), Par. Nos. [0014] to [0021], [0057] to [0071], [0080]; Figs. 1, 5, 6 & US 2003/0097575 A	1-3, 6-8, 11-13, 16, 17, 20, 21
Y		4, 5, 9, 10, 14, 15, 18, 19, 22, 23
Y	JP 11-344925 A (NEC Corp.), 14 December, 1999 (14.12.99), Par. Nos. [0016] to [0042]; Figs. 4 to 11 (Family: none)	4, 5, 9, 10, 14, 15, 18, 19, 22, 23
Y	JP 4-163768 A (Hitachi, Ltd.), 29 October, 1990 (29.10.90), Page 4, left column, line 10 to lower right column, line 13; Figs. 3, 7 (Family: none)	5, 10, 15, 19, 23

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
26 April, 2004 (26.04.04)

Date of mailing of the international search report  
18 May, 2004 (18.05.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl<sup>7</sup> G11B20/10, G11B20/12, G09C1/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl<sup>7</sup> G11B20/10, G11B20/12, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2002-158654 A (株式会社日立製作所) 2002.05.31, 段落【0014】-【0021】、【0057】-【0071】、【0080】、図1, 5, 6 & US 2003/0097575 A	1-3, 6-8, 11-13, 16, 17, 20, 21
Y		4, 5, 9, 10, 14, 15, 18, 19, 22, 23

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」口頭による開示、使用、展示等に言及する文献  
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」同一パテントファミリー文献

国際調査を完了した日

26.04.2004

国際調査報告の発送日

18.5.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

3365

電話番号 03-3581-1101 内線 3597



## C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 11-344925 A (日本電気株式会社) 1999. 12. 14, 段落【0016】 - 【0042】 , 図4-11 (ファミリーなし)	4, 5, 9, 10, 14, 15, 18, 19, 22, 23
Y	JP 4-163768 A (株式会社日立製作所) 1990. 10. 29, 第4頁左欄第10行-右下欄第13行, 図3, 7 (ファミリーなし)	5, 10, 15, 19, 23